Department of Budget and Management
Office of Information Technology

Information Technology
Security Policy and Standards
Version 1.1

July 2003

Approval Date: June 6, 2003
Approved By: James C. DiPaula
Secretary Department of Budget and Management
Distribution: Executive Branch Chief Information Officers
Initiated By: State Data Security Committee

STATE OF MARYLAND
INFORMATION TECHNOLOGY SECURITY POLICY & STANDARDS

1 Information Technology Security Policy 3
2 Key Definitions 5
3 Responsibility Standard 8
4 Information Technology Security Program Standard 10
5 Nonpublic Information Standard 12
6 Access Control Standard 13
7 Network Security Standard 16
8 Physical Security Standard 19
9 Microcomputer/PC/Laptop Security Standard 21
10 Encryption Standard 23
11 IT Information Security Deviation/Risk Acceptance Standard 24
12 Use of Electronic Communications Standard 25
13 Standards Self-Assessment Checklist 26
14 Record of Revisions 32

STATE OF MARYLAND
INFORMATION TECHNOLOGY SECURITY POLICY & STANDARDS

Introduction

This document provides policy and supporting standards for information technology security. The policy applies to Executive agencies of the State of Maryland. It establishes general requirements and responsibilities for protecting technology systems, including the responsibility for each agency to have its own technology security plan. The standards establish minimum levels of compliance.

The policy covers such common technologies as computers, data and voice networks, wireless systems, web systems, and many other more specialized resources. The policy is necessitated by the State government's use of information technology to help carry out nearly all of its public services and internal operations. The State's delivery of critical public services depends on availability, reliability and integrity of its information technology systems. Therefore each agency must adopt appropriate methods to protect its technology systems. While some agencies will need to adopt stronger standards and methods, the statewide program based on this policy provides the minimum requirements and a consistent approach for security.

The common security approach also supports compatible security solutions shared among agencies, yielding a better return on technology investment. The security policy and standards will evolve and will require regular updates to remain current.

The policy and standards are issued by the Secretary of Budget and Management under authority granted by the Annotated Code of Maryland, Finance and Procurement Article § 3-401 through 3-413 and § 3-701 through 3-705. It is administered by the Office of Information Technology within the Department of Budget and Management.

Persons with questions or needing further information are encouraged to contact the Information Technology Security Officer in the Office of Information Technology (410-260-7663).

STATE OF MARYLAND
INFORMATION TECHNOLOGY SECURITY POLICY & STANDARDS

Date Adopted	June 2003
Date of Last Revision	

1 Information Technology Security Policy

Information and information technology systems are essential assets of the State of Maryland. They are vital to the citizens of the State. Information assets are critical to the services that agencies provide to citizens, businesses, and educational institutions, as well as, to local and federal government entities and to other State agencies. All information created with State resources for State operations is the property of the State of Maryland. All agencies, employees, and contractors of the State are responsible for protecting information from unauthorized access, modification, disclosure and destruction.

Each agency of the Executive Branch of the State is responsible for compliance with this policy and these standards. The Office of Information Technology (OIT) of the Department of Budget and Management and agency Information Technology (IT) components are to use this policy and these standards as a guide when procuring information technology services, service providers, contractors, software, hardware and network components.

1.1 Scope

This policy covers all information that is electronically generated, received, stored, printed, filmed, and typed. In accordance with the Annotated Code of Maryland, State Finance and Procurement Article, Section 3-401 through 3-413 and Section 3-701 through 3-705, and with the Executive Order 01.01.1983.18 Privacy and State Data System Security Paragraph 4.D, the provisions of this policy apply to:

- All units of the Executive Branch of the State of Maryland for all of their IT systems regardless of who is operating them
- All activities and operations required to ensure data security including facility design, physical security, disaster recovery and business continuity planning, use of hardware and operating systems or application software, data disposal, and protection of copyrights and other intellectual property rights

1.2 Objectives

This policy and these standards define the minimum requirements to which each State agency, including employees and contractors, must adhere. The primary objectives of the IT Security Policy are:

- To establish a secure environment for the processing of data
- To reduce information security risk
- To communicate the responsibilities for the protection of information

1.3 Previous Policy Superseded

This policy and these standards supersede the policies and standards as previously stated in the “State Agency Data Systems Security Practices” as revised (1999).

1.4 Authority

The State Data Security Committee and the Office of Information Technology of the Department of Budget and Management have authority to set policy and provide guidance and oversight for security of all IT systems in accordance with the Annotated Code of Maryland, State Finance and Procurement Article, Section 3-401 through 3-413 and Section 3-701 through 3-705, and as provided by Executive Order 01.01.1983.18 Privacy and State Data System Security Paragraph 4.D.

1.5 Compliance

The head of each agency is responsible for compliance with and enforcement of this Policy.
Agency Chief Information Officers (CIOs) shall develop and implement an Agency IT Security Program to implement this policy and these standards. The Security Program shall include a timetable and controls for compliance. The controls shall include but are not limited to:

- Maintaining the confidentiality, integrity, availability, and accountability of all State information technology applications and services
- Protecting information according to its sensitivity, criticality and value, regardless of the media on which it is stored or automated systems that process it, or the methods by which it is distributed
- Ensuring that risks to information security are identified and controls implemented to mitigate these risks
- Implementing processes to ensure that all security services meet the minimum requirements set forth in this policy and the attached standards
- Ensuring that all employees and contractors understand and comply with this Policy, as well as all applicable laws and regulations
- Implementing physical security controls to prevent unauthorized and/or illegal access, misuse, destruction or theft of the State's IT assets

1.6 Security Program Maintenance and Review

Each State agency will review and update its IT Security Program as needed to conform to changes within the agency or in the State IT Security Program. IT Systems security plans will be reviewed as required by IT security Certification and Accreditation guidelines.

1.7 Information Technology Security Deviation and Risk Acceptance

Compliance with this policy shall be planned and achieved as promptly as possible. When an agency determines, in the course of planning or carrying out its IT Security Program, that it is not feasible or practical to comply with a provision or provisions of this policy and attendant standards, or to do so promptly, it shall document the deviation from policy or standards. The documentation, with a timetable for compliance when practicable, shall be prepared as an IT Security Deviation Request.

IT Security Deviation Requests must be filed in accordance with the specifications detailed in the State IT Security Deviation/Risk Acceptance Standard (see section 11, IT Security Deviation/Risk Acceptance Standard). Such deviations require the approval of the agency CIO and the State CIO.

Date Adopted	June 2003
Date of Last Revision	

2 Key Definitions

Term / Acronym	Definition
Acceptable Risk	A vulnerability that is acceptable to responsible management, due to the cost and magnitude of implementing countermeasures.
Accountability	A system's ability to determine the actions and behavior of a single individual within a system, and to identify that particular individual.
Accreditation	The authorization and approval granted to operate a system or network in order to process sensitive data in an operational environment.
Agency	All units of the Executive branch excluding the University System of Maryland.
Authentication	The testing or reconciliation of evidence of a user's identity.
Authorization	The rights and permissions granted to an individual (or process), which enables access to a computer resource.
Authorized Software	Software owned or licensed and used in accordance with the software license or software approved for use by the agency for a specific job function.
Availability	Ensures the reliable and timely access to data or computing resources by the appropriate personnel.
Certification	A technical review made as part of and in support of the accreditation process. Certification shows the extent to which a particular computer system or network design and implementation meets a pre-specified set of security requirements. A judgment and statement of opinion that the accrediting official can use to officially accredit the system is produced.
CIO	Chief Information Officer.
Cold Site	An alternate facility that is void of any resources or equipment except air-conditioning and raised flooring. Equipment and resources must be installed to duplicate the critical systems.

Term / Acronym	Definition
Computer	An electronic, magnetic, optical, or other data processing device or system that performs logical, arithmetic, memory, or storage functions. It includes any data storage facility, or communications facility that is directly related to or operated in conjunction with that device or system.
Confidentiality	Restriction from disclosure, intentionally or unintentionally, to unauthorized persons, processes or devices.
Data Remanence	Residual information left behind once media has been in some way erased.
Incident	Any event, suspected event or attempted action that could pose a threat to the integrity, availability, confidentiality, or accountability of an IT System. Incidents include an attempted security breach, IT System disruption or outage.
Identification	Data uniquely labeling a user to a system.
IDS	Intrusion Detection System
Information Custodian	The business function owner responsible for the information assets for a particular IT System
Integrity	Freedom from corruption or unauthorized modification; internal and external consistency.
IT Systems	Automated systems: communications systems including wireless systems, computer systems, hardware and software, application systems, networks, workstations, servers, personal digital assistants and data on the IT System.
ITEPP	Information Technology Emergency Preparedness Plan, including the business continuity plan, the recovery plan and the business resumption plan.
MCERT	Maryland's Computer Emergency Response Team. Team to be activated in the event of a major IT related disaster.
Network	A system containing any combination of computers, computer terminals, printers, audio or visual display devices or telephones interconnected by telecommunications equipment or cables, used to transmit or receive information.

Term / Acronym	Definition
NIST	National Institute of Standards and Technology.
Non-repudiation	Authentication with a high assurance to be genuine and that can not subsequently be refuted.
OIT	Office of Information Technology within the Department of Budget and Management
Perimeter Access	Access to all entry and exit points of the network, controlled by firewalls and other filtering mechanisms.
Policy	For purposes of this document means both Policy and Standards
PPI	Proprietary and/or Protected Information is information that is not subject to inspection and copying under the Maryland Public Information Act or federal law.
Privacy	The level of confidentiality and protection that a user is given in a system.
PUB	Public Information means information that may be inspected and copied under the Maryland Public Information Act. .
Residual Risk	The portion of risk that remains after security measures have been applied.
Risk	The probability that a particular threat will exploit a particular vulnerability of an IT System.
SDLC	Systems Development Life Cycle as defined in the State of Maryland SDLC Methodology (See www.dbm.state.md.us/html/sdlc.html.)
Software	Computer programs, instructions, procedures, or associated documentation that is concerned with the operation of a computer system.

Date Adopted	June 2003
Date of Last Revision	

3 Responsibility Standard

The following standard sets the minimum level of responsibility for the following individuals and/or groups:

- State Data Security Committee
- State CIO
- Division of Security and Architecture for OIT
- Agency
- Employees and Contractors

3.1 State Data Security Committee

The responsibilities of this committee are outlined in the Executive Order 01.01.1983.18 Privacy and State Data System Security. The committee:

- Is the governance body mandated by Executive Order to control data security
- Will evaluate the security of State agency systems containing computerized records
- Defines IT system security measures to be undertaken
- Monitors, through agency self assessment, compliance with the current policy
- Reports to the Governor and the Legislative branch the status of data security

3.2 State Chief Information Officer

The duties of the State CIO are:

- Providing Statewide IT security policy, standards, guidelines, and procedures
- Ensuring the State's IT Security Program is established and implemented in compliance with State laws and regulations and federal laws where applicable
- Approving deviations to IT security requirements
- Reporting to the Governor and the Legislature on the status of the State's IT Security Program
- Enforcing State security policy, including establishing the appropriate measures and remedial actions for agencies for non-compliance

3.3 Division of Security and Architecture, DBM OIT

The division is responsible for**:**

- Developing and maintaining a Statewide Security Program that includes policy, standards, guidelines, procedures, best security practices, IT disaster recovery planning guidelines, IT Security Certification and Accreditation guidelines, security awareness training, and an incident response reporting capability
- Identifying security vulnerabilities in State systems and recommending corrective action
- Ensuring IT Disaster Recovery plans for critical IT Systems are maintained and that plans are exercised at least annually
- Developing and maintaining a Statewide security architecture
- Coordinating with State Agencies' CIO, federal and local government, and private industry to resolve security issues and improve security for State systems.

- Provide the appropriate guidance to assist agencies in establishing IT Security Programs and compliance with IT Security Policy
- Working with other State agencies to establish a coordinated computer incident response effort.

3.4 Agency Responsibilities

Each agency is responsible for:

- Ensuring the agency's IT Security Program is established and implemented in compliance with State security policies and standards, State and federal laws and regulations as applicable
- Implementing a IT Security Certification and Accreditation process for the life cycle of each agency IT System
- Reporting to the OIT on the status of the agency's IT Security Program
- Enforcing the State IT Security Policy
- Managing the program and initiating measures to assure and demonstrate compliance with security requirements
- Assuring the confidentiality, integrity, availability, and accountability of all agency information while it is being processed, stored, and/or transmitted electronically, and the security of the resources associated with the processing functions
- Assuming the lead role in resolving security and privacy incidents
- Documenting and ensuring that a process is implemented for the classification of information in accordance with the Information Sensitivity and Classification Standard
- Specifying the level of security required to protect all information assets under their control to comply with this Policy
- Generating any IT Information Security Deviation in accordance with the standard
- Assuring that an IT disaster recovery plan has been implemented in accordance with the IT Disaster Recovery Plan Guidelines
- Development, implementation and testing of the IT Disaster Recovery Plan for critical agency IT Systems
- Ensuring a configuration/change management process is used to maintain the security of the IT system
- Administering a virus prevention and incident reporting program that coordinates with Maryland’s Computer Incident Response Team
- Ensuring separation of duties and assigning appropriate system permissions and responsibilities for agency system users

3.5 Employees and Contractors

All employees and contract personnel are responsible for:

- Being aware of their responsibilities for protecting IT assets of their agency and the State
- Exercising due diligence in carrying out the IT Security Policy
- Being accountable for their actions relating to their use of all IT Systems
- Using IT resources only for intended purposes as defined by policies, laws and regulations of the State

Date Adopted	June 2003
Date of Last Revision	

4 Information Technology Security Program Standard

Each agency is responsible for developing an IT Security Program for securing the agency's communications systems, computer systems, networks, and data in accordance with the State IT Security Policy. The status of an agency It Security Program will be reported to the State CIO on an annual basis in conjunction with the Annual Data Security Survey. This standard specifies the major components that must be included in every IT Security Program. The following list is not exhaustive; it functions as the minimum set of requirements. At a minimum each program must contain the following elements:

- IT Security Policy
- Risk Management
- Systems Development Life Cycle Methodology
- IT Security Certification and Accreditation
- IT Disaster Recovery Planning
- IT Security Awareness Training
- IT Incident Response Process
- External Connections Review
- IT Security Plan Reporting.

4.1 IT Security Policy

Each agency must adopt or develop an agency IT security policy, with standards, and procedures. Policy must meet the minimum requirements as set forth in this Policy.

4.2 Risk Management

A risk management process must be implemented to assess the acceptable risk to agency IT Systems as part of a risk-based approach used to determine adequate security for the system. Agencies shall analyze threats and vulnerabilities and select appropriate, cost-effective controls to achieve and maintain a level of acceptable risk. Agencies will define a schedule for on-going risk management review and evaluation based on the system sensitivity and data classification of the system (see section 5, Nonpublic Information Standard). Refer to NIST Special Publication 800-30 Risk Management Guide for Information Technology at, http://csrc.nist.gov/publications/nistpubs/ for guidance.

4.3 Systems Development Life Cycle Methodology

All State systems must include IT security as part of the system development life cycle management process. Refer to the requirements in the State of Maryland SDLC Methodology (See http://www.dbm.maryland.gov/communities/community.asp?UserID=2&CommunityID=226&Folder=2512)

4.4 IT Security Certification & Accreditation

Agencies shall develop and implement an IT security certification and accreditation program as part of an overall IT risk management strategy. The program will maintain a catalog of all IT systems and sites (to include existing), ranked by sensitivity and criticality. The cataloged items should be certified and accredited, in order, according to the State IT Security Certification and Accreditation (C&A) Guidelines. All new development shall be conducted using the IT Security C&A process integrated into the development process. (See the State IT Security Certification and Accreditation Guidelines)

4.5 IT Disaster Recovery Planning

Agencies shall develop, implement, and test an IT Disaster Recovery plan for each critical IT system to ensure that a contingency system will be available in the event of a disaster to the primary production system. (See the State IT Disaster Recovery Guidelines)

4.6 IT Security Awareness, Training, and Education

Agencies shall develop and implement a security awareness, training, and education program for all agency employees and contractors to ensure that all employees and contractors adhere to the State IT Security Policy. (See the State IT Security Awareness Training and Education Training Guidelines)

4.7 IT Incident Response Process

Agencies shall be required to participate in the State Incident Response Process by detecting, tracking, logging, and reporting security incidents. (See the Maryland Computer Incident Response Capability Procedures and the Standard Operation Procedures for Electronic Evidence Handling)

4.8 External Connections Review

External network connections, non-networked computers and dial-in connections shall be managed, reviewed annually, and documented as prescribed by the Agency IT Security Program. Results will be reported annually as part of the IT security assessment transmitted to the Office of the State CIO and to the SDSC.

4.9 IT Security Plan Reporting

Each agency is responsible for reporting on the status of the agency IT Security Program to the State Data Security Committee and the DBM/OIT Division of Security and Architecture on an annual basis. A project plan detailing the projects, estimated costs, and estimated completion time required to bring the agency into compliance with the IT Security Policy must be included in the annual report.

Date Adopted	June 2003
Date of Last Revision	

5 Nonpublic Information Standard

Agencies shall establish and document a process that protects nonpublic information from disclosure to unauthorized individuals or entities, including other State or federal agencies. The process shall be compliant with the Maryland Public Information Act and any applicable federal laws.

5.1 System Sensitivity Designation

Each agency must specify corresponding classification and controls that must be in place for the data within that agency. When the IT System is shared between State units and/or between State, Federal, or local units the highest level of classification will determine the classification of the data or IT System. For example, one agency may categorize the data at a medium level while the second agency may classify the data at a basic level, therefore, the data at both agencies will be at a medium level. All parties sharing the IT System or data must agree to the initial classification and any change in the classification. An IT System shall clearly identify data that is considered PPI and any electronic exchange of data will clearly state that the information is PPI.

Date Adopted	June 2003
Date of Last Revision	

6 Access Control Standard

All Agencies must ensure that information is accessed by the appropriate persons for authorized use only. To help accomplish this each agency must establish at a minimum the following:

- An authentication process to verify the identity of users prior to initiating a session or transaction on an IT system
- An authorization process which specifically grants access to information ensuring that access is strictly controlled, audited, and that it supports the concepts of "least possible privileges" and " "need-to-know"
- An audit trail process to ensure accountability of system and security-related events
- A process for ensuring that all systems have the ability to log and report specific security incidents and all attempted violations of system security. In addition, this capability must be enabled at all times
- A review process of security audit logs, incident reports and on-line reports at least one (1) time per business day
- An investigation process for any unusual or suspicious items, which will incorporate reporting the results as specified in the State IT Incident Response Guideline
- An internal assessment process for verifying their compliance to the State IT Security Policy
- The processes to establish, manage, and document user id and password administration
- A review of access privileges on an annual basis
- A process for protecting nonpublic information
- A process for explicitly authorizing access to nonpublic information
- A process for documenting and escalating all instances of non-compliance with the State IT Security Policy
- A segregation of the functions of system administration and security administration to provide separation of duties
- Procedures prohibiting security personnel from initiating, programming, processing or authorizing business transactions
- Independent audits of agency security administrators security transactions

6.1 Authentication

All users must be uniquely identified. Group or shared ids are prohibited unless they are documented as "Functional ids". Functional ids are user accounts associated with a group or role that may be used by multiple individuals (e.g.. Emergency Problem/Fix Ids) or that are associated with a particular production job process (e.g., RACF id used to run production jobs). Passwords associated with functional ids are exempt from the password restriction on sharing and change requirements specified below.

Password Construction Rules and Change Requirements

Passwords must meet the following usage, construction and change requirements:

- The password must not be the same as the user id
- Passwords must never be displayed on the screen

- The user must select passwords unless randomly generated. Initial passwords and password resets distributed to the user must be issued "pre-expired" forcing the user to change them upon logon
- Passwords must be a minimum of eight (8) characters and consist of mixed alphabetic and numeric characters. Passwords must not consist of all numbers, all special characters, or all alphabetic characters
- Passwords must not contain leading or trailing blanks
- Passwords must not contain more than two (2) consecutive identical characters
- Password reuse must be prohibited for a minimum of six (6) months.
- Where possible, users should be prohibited from only changing/or adding one (1) character to their previous password (i.e., users should be prohibited from using passwords that are similar to their previous password)
- Automated controls must ensure that passwords are changed at least as frequently as every forty-five (45) days
- Passwords older than its expiration date must be changed before any other system activity is performed
- User ids associated with a password must be disabled after not more than four (4) consecutive failed login attempts and require security administration to reactivate the id
- When a user password is reset or redistributed, the validation of the user identity must be at least as strong as when originally established

6.2 Authorization

All Agencies must have the following authorization controls implemented:

- A documented process to ensure that access privileges are verified at least annually
- An automated process to ensure that individual user sessions either time out or initiate a password protected screen saver after a period of thirty (30) minutes of inactivity
- A documented process to ensure that access rights reflect changes in employee/contractor status within twenty-four (24) hours of the change
- A documented process to ensure that physical and logical access is immediately disabled upon a change in employment status where appropriate
- An automated process to ensure that user ids are disabled after sixty (60) days of inactivity and deleted after ninety (90) days of inactivity unless they are extended through the explicit approval of the Information Custodian (Note: Functional ids may be exempted from this requirement)
- A documented process to ensure that all default access capabilities are removed, disabled, or protected to prevent unauthorized use
- A process/system to ensure that access privileges are traceable to a unique user id
- An automated display, after a successful logon, showing the date and time of last successful logon and the number of unsuccessful logon attempts since the last successful logon

6.3 Audit Trail

The following minimum set of events/actions must be logged and kept as required by State and Federal laws/regulations:

- Additions, changes or deletions to data produced by IT systems
- Identification and authentication processes

- Actions performed by system operators, system managers, system engineers, technical support, and system administrators
- Emergency actions performed by support personnel and highly privileged system and security resources

The audit trails must include at least the following information:

- Date and time of event
- User id of person performing the action
- Type of event
- Asset or resource name and type of access
- Success or failure of event
- Source (terminal, port, location, and so forth) where technically feasible

In addition, all lapses in audit trails must be immediately investigated by security administration and the Information Custodian and brought to closure within one (1) week.

6.4 Violation Log Management and Review

The Information Custodian must review all violations within one business day of a discovered occurrence. At a minimum the following events should be reviewed:

- Two (2) or more failed attempts per system day to access or modify security files, password tables or security devices
- Disabled logging or attempts to disable logging
- Two (2) or more failed attempts to access or modify nonpublic information within a week
- Any unauthorized attempts to modify software or to disable hardware configurations

Date Adopted	June 2003
Date of Last Revision	July 2003

7 Network Security Standard

Agencies must ensure that all information networks are protected from unauthorized access at all entry points. To help accomplish this each agency must, at a minimum:

- Establish a process to protect from unauthorized dial-in access
- Utilize the State approved banner text (See 7.2)
- Establish a process to ensure that all external IP connections are made through a firewall
- Implement and monitor an Intrusion Detection Systems (IDS) 24X7X365
- Establish a process to ensure that all Service Interface Agreements (SIAs) are managed in accordance with their IT Security Program and the State Policy
- Establish a process to ensure that the same level of controls that exist on-site exist for users working remotely
- Establish a process to prevent unauthorized mobile code from being loaded onto State IT equipment
- Establish a process for ensuring that wireless network connections do not compromise the State's IT Security Program
- Establish a process for securing all Private Branch Exchanges (PBXs)

7.1 Dial-in Access

The following services are prohibited except where they are specifically approved by the Agency CIO:

- Dial-in desktop modems
- Use of any type of "remote control" product (e.g., PCAnywhere)
- Use of any network-monitoring tool

In addition, the following controls for dial-in users must be implemented:

- Unique network access user ids different from their application or network user id.
- A minimum prohibition of answer or pickup until after the sixth (6^{th}) ring
- Access privileges must be prohibited to any applications except those expressly required (i.e., cannot grant access to entire network, must be application specific)
- Annual review of access requirements
- Shall not store data unless the data can be protected from unauthorized access, modification, or destruction

7.2 Banner Text

The following banner text must be displayed at all system entry points and at all access points to servers, subsystems, etc. where initial user logon occurs:

> *"Access to this system is restricted to authorized users only and limited to approved business purposes. By using this system, you expressly consent to the monitoring of all activities. Any unauthorized access or use of this system is prohibited and could be subject to criminal and civil penalties. All records, reports, e-mail, software, and other data generated by or residing upon this system are the property of State of Maryland and may be used by the State of Maryland for any purpose."*

An automatic pause, slow roll rate, or user acknowledgement is required to ensure that the banner can be read. The banner is:

- Required for all mainframe, midrange, workstation, personal computer, and network systems
- Must be used in addition to, and is not a substitute for, any default banners or copyright/proprietary notices
- The first banner that is displayed, except for citizen interfaces where use will negatively impact the citizen. In such cases, this negative impact must be documented by management

7.3 Firewalls & Network Devices

State networks will be protected by firewalls at identified points of interface as determined by system sensitivity and data classification. State firewalls should be configured to block all services not required and disable unused ports, hide and prevent direct accessing of State trusted network addresses from untrusted networks, maintain comprehensive audit trails, fail in a closed state and operate on a dedicated platform (device).

All network devices (e.g. servers, routers) shall have all non-needed services disabled and the security for those devices hardened. All devices shall have updates and patches installed on a timely basis to correct significant security flaws. Default or initial passwords shall be changed upon installation of all firewall and network equipment.

7.4 Intrusion Detection Systems

State networks will be monitored by an IDS implemented at critical junctures. Host-based, network-based, or a combination of both (preferred) may be utilized. IDS must be monitored 24X7X365. Each agency must establish a severity and escalation list based upon anticipated events that include immediate response capability when appropriate. These plans should be incorporated into the Agency's IT Security Program.

7.5 Service Interface Agreement

External network connections shall be permitted only after all approvals required by State law are obtained and shall be managed in accordance with a Service Interface Agreement (SIA) that is agreed to by the State agency and the non-State entity. These connections are subject to the Maryland Public Information Act and should not be part of the ordinary process of doing business. Specific criteria should be included in the system It Security Certification and Accreditation package in the IT System security plan. An SIA shall include:

- Purpose and duration of the connection as stated in the agreement, lease, or contract
- Points-of-contact and cognizant officials for both the State and non-State organizations
- Roles and responsibilities of points-of-contact and cognizant officials for both State and non-State organizations
- Security measures to be implemented by the non-State organization to protect the State's IT assets against unauthorized use or exploitation of the external network connection
- Requirements for notifying a specified State official within a specified period of time of a security incident on the network, with the recommended time within 4 hours of the incident
- A provision allowing the State to periodically test the ability to penetrate the State's network through the external network connection or system

7.6 Teleworking

In a telecommuting environment, an agency must require the same level of security on the microcomputer used at home or offsite as the microcomputer used in the workplace.

7.7 Mobile Code

Until reliable executable content scanning technology is available to address security concerns with regard to mobile code or executables obtained via the Web, all mobile code or executable content employed within a agency intranet shall be documented in the IT System Security Plan and approved by the Agency CIO.

7.8 Wireless Networks

Should agencies establish addressable network segments for the wireless networks, they must ensure that they do not compromise the State IT Security Program. All such networks must at a minimum incorporate the following controls:

- Properly configuring of routers
- Encrypting the wireless transmissions using 128 bit Virtual Private Networks (VPNs)
- Authenticating users with user validation mechanisms more secure than passwords only
- Changing the default service set identifier (SSID)
- Disabling “broadcast SSID”

7.9 Private Branch Exchange (PBX)

If PBX processors require remote vendor maintenance via a dial-in telephone line the following controls must be in place:

- A single dedicated telephone line that disables access to the public-switched telephone network
- An automated audit trail
- Encryption of transmissions
- Access controls

7.10 Facsimile

Data transmitted by facsimile must be treated in the same manner as any data communicated by network or PBX based on system sensitivity and data classification.

Date Adopted	June 2003
Date of Last Revision	

8 Physical Security Standard

Physical access to IT information processing, storage areas, and storage devices and its supporting infrastructure (communications, power, and environmental) must be controlled to prevent, detect, and minimize the effects of unauthorized or unintended access to these areas. Agencies must:

- Secure IT areas with controls commensurate to the risks
- Ensure the secure destruction storage media
- Ensure secure media reuse
- Ensure secure storage of media
- Obtain personnel security clearances where appropriate

8.1 Secured IT Areas

Physical access controls must in place for the following:

- Data Centers
- Areas containing servers and associated media
- Networking cabinets and wiring closets
- Power and emergency backup equipment
- Operations and control areas

Access to data centers and secured areas will be granted for those employees, contractors, technicians and vendors who have legitimate business responsibilities in those areas. Authorization should be:

- Based on frequency of need for access
- Approved by the manager responsible for the secured area

Each agency is responsible for:

- Issuing picture id badges to all Employees/contractors and ensuring that these badges are openly displayed at all times
- Ensuring that all portable storage media such as hard drives, diskettes, magnetic tapes, laptops, and CD are physically secured
- Ensuring proper environmental and physical controls are established to prevent accidental or unintentional loss of information residing on IT systems
- Ensuring that any physical access controls are auditable

8.2 Storage Media Disposal

When no longer usable diskettes, compact disks, tape cartridges, ribbons, and other similar items shall be destroyed by a NIST approved method such as shredding, incineration, overwriting, or degaussing. All IT equipment shall not be released from an agency's control until the equipment is sanitized and all stored information has been cleared. This requirement applies to all permanent disposal of equipment regardless of the identity of the recipient. This includes equipment transferred to schools, as well as equipment maintenance and repair.

8.3 Media Reuse

When no longer required for mission or project completion, media (tapes, disks, hard drives, etc.) to be used by another person within the agency shall be overwritten with software and protected consistent with the data sensitivity at which IT storage media were previously used. The procedures shall be documented in the IT System Security Plan.

8.4 Storage And Marking

IT Systems and electronic media shall be protected and marked in accordance with the data sensitivity. Users shall not store data on electronic media that cannot be adequately secured against unauthorized access.

8.5 Personnel

Security clearances are required for personnel as determined by the system sensitivity and data classification designation. Agencies will ensure that an appropriate background investigation (e.g., CJIS, State Police) has been completed on personnel as necessary. Agencies will maintain personnel clearance information on file.

Date Adopted	June 2003
Date of Last Revision	

9 Microcomputer/PC/Laptop Security Standard

Agencies must ensure that all microcomputer (i.e., workstation, desktop computers, laptops computers, PDA's, and any other portable device that processes data) are secured against unauthorized access. The level of controls should be commensurate with the information accessed, stored, or processed on these devices. To help accomplish this each agency must establish at a minimum the following:

- General controls
- Virus protection
- Software licensing and use controls
- Laptop security and mobile computing controls
- Protection from personally owned microcomputers

9.1 General Controls

All microcomputers that store and/or access nonpublic information must implement the following controls:

- User id and password to control access at logon
- Encryption to protect directories, sub-directories, and/or files containing nonpublic information
- Virus Protection

Standard virus protection programs must be installed, updated, and maintained on all microcomputers, LAN servers, and mail servers. These programs must:

- Be configured to run checks for viruses at startup and operate in memory-resident mode to check for viruses during normal processing
- Be updated as soon as updates are available from the vendor
- Be configured to prevent connection to the network unless the accessing microcomputer has the latest version of the virus product and update installed

9.2 Software Licenses And Use

Agencies shall establish procedures to ensure compliance with State Copyright Policy, Department of Budget and Management Policy Number 95-1, and assure that software installed on agency IT Systems is incorporated into the SDLC management process.

Unless specifically approved by the Agency CIO and the agency head, personal or corporate IT equipment shall not have State licensed software installed and shall not be used to process or transmit PPI. Only State owned and authorized computer software is to be used on standalone or networked computer equipment.

Authorized software packages are those approved by the Agency CIO. Executable modules cannot be downloaded from the Internet unless authorized by the Agency CIO and agency network administrator. Agencies should designate a single point of contact for inquiries about copyright violations, pursuant to federal law.

9.3 Laptop Security And Mobile Computing

Laptops and mobile computing devices are not authorized to process or store nonpublic information unless approved in writing by the agency network support administrator, the Agency CIO and the agency head. Laptops and mobile computing devices which include personal digital assistants approved for processing PPI information cannot be connected to State networks or systems unless the network or system is certified and accredited for that function. In such cases the IT Security Program will identify the devices that can be used to access the network or the system, the purposes for the access, and the security controls for the connection.

9.4 Personally Owned Data Processing Equipment

Processing or storing PPI on personal or contractor owned data processing equipment is prohibited unless approved by the agency network support administrator, the Agency CIO and the agency head.

Date Adopted	June 2003
Date of Last Revision	

10 Encryption Standard

Agencies must ensure that encryption is utilized to protect any non-public information when it is stored or transmitted through any environment. IT Systems employing encryption must comply with all applicable Federal Information Processing Standards (FIPS) publications and guidelines for encryption (References located at http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf),

To help accomplish this each agency using encryption must establish at a minimum the following:

- Secure cryptographic keys
- Use of Public Key Cryptography methods approved by the State CIO
- All cryptographic keys must have a designated, unique owner.

Key change intervals shall be established by each agency, but must be no longer than the following:

- Master keys must be changed once per year, if the product allows
- Key encrypting keys (e.g., asymmetric encrypting a symmetric) must be changed at a minimum of every six (6) months
- Link encrypting keys must be changed every thirty (30) days

Keys must be distributed in a secure manner ensuring that the entire key is not exposed while in transit to any one individual at any one time.

Default cryptographic keys may not be utilized, except they may be utilized for emergency recovery, system calibration or vendor certification purposes. In such cases, a documented process describing the storage, maintenance, use and destruction of these keys must be in place.

10.1 Public Key Technology (Asymmetric)

All public key management systems, Certification Authorities (CAs), key distribution systems, key recovery systems, and cross-certification processes must be approved by the State CIO and the State Data Security Committee. Every public key and certificate must have an associated scope of use, which must be checked by any user or server that accepts or relies upon the certificate.

The process for issuing digital certificates must:

- Establish the identity of the subject
- Establish that the subject is the holder of the associated private keys

Date Adopted	June 2003
Date of Last Revision	

11 IT Information Security Deviation/Risk Acceptance Standard

An Information Security Deviation Request/Risk Acceptance form must be completed by the agency if it determines that it cannot or will not comply with the State IT Security Policy. All deviation requests require the approval of the agency CIO, Information Custodian, agency head, and the State CIO.

11.1 General Requirements

- Proposed deviations will be considered on an individual basis
- Where appropriate, a risk assessment will be performed to evaluate the threats, countermeasures and extenuating circumstances associated with the proposed deviation and its impact on IT systems
- Requests for deviations must by completed by the requesting Information Custodian and must be made in writing
- Deviations will be granted for a maximum period of twelve (12) months after which time the deviation will be considered expired and require renewal by the Information Custodian

Date Adopted	June 2003
Date of Last Revision	

12 Use of Electronic Communications Standard

This standard applies to information technology security, however, it is not inclusive of other State policies and regulations that may further apply to the use of electronic communications.

The use of the Internet, E-mail and other State computing equipment, networks and communication facilities is provided to State employees and contract employees as electronic tools to perform their job functions. Information communicated electronically through email, the Internet or sharing of electronic documents is subject to State laws, regulations, policies and other requirements, as is information communicated in other written forms and formats. Access to State agency email or Internet services may be wholly or partially restricted without prior notice and without user consent.

12.1 Internet and Electronic Communications

Users accessing the Internet or other State electronic communications through State resources may be monitored. Agencies shall develop standards consistent with all State policies and standards regarding E-mail, Internet use, and use of other computer resources. Electronic communications that are not secure or encrypted should not be used to send information that is nonpublic information.

12.2 Computer Software

Users, unless specifically authorized because of their job functions, are not permitted use unauthorized software (e.g., downloaded software, pirated software, software not licensed to the State, software brought from home). This includes, but is not limited to programs, executable modules and screen savers. (*Refer to additional guidance in the State of Maryland Software Code of Ethics Form, Department of Budget and Management's Policy Number 95-1)*

12.3 IT Incident and Advisories

Each agency shall notify its staff of the personnel designated to provide authenticated notices of IT incidents and advisories. Employees other than the designated personnel shall not forward IT Incident advisories to agency staff. If an advisory comes to an employee, the employee shall forward it to the designated personnel for evaluation.

Date Adopted	June 2003
Date of Last Revision	

13 Standards Self-Assessment Checklist

The purpose of this checklist is to assist individuals designing new application, architectures, or modifying existing systems. The checklist is designed to provide questions pertaining to the majority of the IT Security Standards. It does not include many of the administrative functions detailed in the IT Security Standards and it should not be considered a substitute for reading the IT Security Policy. The checklist had been designed so that an answer of "NO" indicates a potential security issue that requires further investigation.

	IT Security Program Standard	N/A	Yes	No
1.	Does the agency have an IT Security Program? *(Section 4)*			
2.	Has the agency adopted the State IT Security Policy or developed its own policy? *(Section 4.1)*			
3.	Has the agency adopted the State IT Security Standards or developed its own standards? *(Section 4.1*			
4.	Has the agency implemented a risk management process for determining adequate security levels for the IT systems? *(Section 4.2)*			
5.	Is IT security included as part of the SDLC? *(Section 4.3)*			
6.	Has the agency developed and implemented an IT security certification and accreditation program as part of its overall IT risk management strategy? *(Section 4.4)*			
7.	Has the agency developed, implemented, and tested and IT Disaster Recovery plan for each critical IT system? *(Section 4.5)*			
8.	Has the agency developed and implemented a security awareness, training, and education program for all agency employees and contractors? *(Section 4.6)*			
9.	Is the agency participating in the State Incident Response Process? *(Section 4.7)*			
10.	Are all external network connections, non-networked computers and dial-in connections documented and reviewed for security implications on an annual basis? *(Section 4.8)*			
11.	Is the agency reporting the status of its IT Security Program to the State Data Security Committee and the DBM/OIT Division of Security and Architecture on an annual basis? *(Section 4.9)*			
	Nonpublic Information Standard			
12.	Has the agency established and documented a process that protects nonpublic information from disclosure to unauthorized individuals or entities? *(Section 5)*			
13.	Has the agency documented a process for protection for nonpublic information? *(Section 5)*			
		N/A	**Yes**	**No**

14.	Has the agency specified the corresponding controls that must be in place for each level of classification? *(Section 5.1)*			
	Access Control Standard			
15.	Is the agency ensuring that information is accessed only by the appropriate persons for authorized use? *(Section 6)*			
16.	Has an authentication process verifying the identity of users prior to initiating a session or transaction been implemented for all systems containing nonpublic information? *(Section 6)*			
17.	Has an authorization process that specifically grants access to nonpublic information that ensures that the access is strictly controlled, audited, and supports the concepts of "least possible privileges" and "need-to-know" been implemented? *(Section 6)*			
18.	Has an audit process been implemented to ensure that accountability of system and security-related events? *(Section 6)*			
19.	Has a process been implemented to ensure that all systems have the ability to log and report specific security incidents and attempted violations? *(Section 6)*			
20.	Is there a segregation of the functions of system administration and security administration providing separation of duties? *(Section 6)*			
21.	Is there an independent verification of security transactions? *(Section 6)*			
22.	Are group or shared ids prohibited? *(Section 6.1)*			
23.	Are passwords prohibited from being the same as the user id? *(Section 6.1)*			
24.	Are passwords prohibited from being displayed in clear-text on the screen? *(Section 6.1)*			
25.	Are initial passwords and password resets distributed to the user in a "pre-expired" state? *(Section 6.1)*			
26.	Are passwords selected by the user or randomly generated? *(Section 6.1)*			
27.	Are passwords required to be a minimum of eight (8) characters? *(Section 6.1)*			
28.	Are passwords required to be a mix of alphabetic and numeric characters? *(Section 6.1)*			
29.	Are passwords prohibited from containing leading or trailing blanks? *(Section 6.1)*			
30.	Are passwords prohibited from containing more than two (2) consecutive identical characters? *(Section 6.1)*			
31.	Are passwords prohibited from being reused for a minimum of six (6) months? *(Section 6.1)*			
32.	Have automated controls been implemented to ensure that passwords are changed at least as frequently as every forty-five (45) days? *(Section 6.1)*			
33.	Are user ids disabled after not more than four (4) consecutive failed login attempts? *(Section 6.1)*			
34.	Do disabled ids require security administration to reactivate the id? *(Section 6.1)*			
35.	Has a documented process been implemented to ensure that access privileges are verified at least			

	annually? *(Section 6.2)*			
36.	Has an automated process been implemented to ensure that individual user sessions either time out or initiate a password protected screen saver every thirty (30) minutes? *(Section 6.2)*			
37.	Has a documented process been implemented to ensure that access rights reflect changes in employee/contractor status within twenty-four (24) hour of the change? *(Section 6.2)*			
38.	Has a documented process been implemented to ensure that physical and logical access is immediately disabled upon a change in status where appropriate? *(Section 6.2)*			
39.	Has an automated process been implemented to ensure that user ids are disabled after sixty (60) days of inactivity? *(Section 6.2)*			
40.	Has an automated process been implemented to ensure that user ids are deleted after ninety (90) days of inactivity? *(Section 6.2)*			
41.	Has a documented process been implemented to ensure that all default access capabilities are removed, disabled, or protected to prevent unauthorized use? *(Section 6.2)*			
42.	Has an automated process been implemented to ensure that access privileges are traceable to a unique id? *(Section 6.2)*			
43.	Has an automated display been implemented showing the date and time of the last successful logon and number of failed logon attempts? *(Section 6.2)*			
44.	Are audit trails maintained as required by Federal or State laws/regulations? *(Section 6.3)*			
45.	Do the audit trails capture all additions, changes, or data produced by IT Systems? *(Section 6.3)*			
46.	Do the audit trails capture all identification and authentication processes? *(Section 6.3)*			
47.	Do the audit trails capture all actions performed by the system operators, system managers, system engineers (technical support), and system administrators? *(Section 6.3)*			
48.	Do the audit trails capture all the emergency actions performed by support personnel and highly privileged system and security resources? *(Section 6.3)*			
49.	Do the audit trails contain the date and time of the event? *(Section 6.3)*			
50.	Do the audit trails contain the user id of the person performing the action? *(Section 6.3)*			
51.	Do the audit trails contain the type of event (e.g., read, update, delete, etc.)? *(Section 6.3)*			
52.	Do the audit trails contain the resource name? *(Section 6.3)*			
53.	Do the audit trails contain the success or failure of the event? *(Section 6.3)*			
54.	Do the audit trails show source (e.g., terminal, port, etc.) where technically feasible? *(Section 6.3)*			
55.	Are all lapses in audit trails immediately investigated by the Information Custodian and brought to closure within one (1) week? *(Section 6.3)*			
56.	Are the violation logs reviewed by the Information Custodian within one (1) business day? *(Section 6.4)*			

	Network Security Standard			
57.	Has a process been established to protect from unauthorized dial-in access? *(Section 7)*			
58.	Is the State approved banner text being presented at all initial login points? *(Section 7)*			
59.	Has a process been implemented to ensure that all external IP connections are protected by a firewall? *(Section 7)*			
60.	Is IDS implemented and monitored 24X7X365? *(Section 7)*			
61.	Has a process been implemented to ensure that all SIAs are managed in accordance with the IT Security Program, Policy, and Standards? *(Section 7 and 7.5)*			
62.	Have controls been implemented to ensure that remote users have the same level of controls that exist onsite? *(Section 7 and 7.6)*			
63.	Have controls been implemented to prevent unauthorized mobile code from being loaded onto State IT equipment? *(Section 7 and 7.7)*			
64.	Has a process been implemented to ensure that any wireless connections do not compromise the State's Security Program? *(Section 7 and 7.8)*			
65.	Have all PBXs been secured? *(Section 7 and 7.9)*			
66.	Have dial-in modems been prohibited except where they are specifically, and uniquely approved by the agency CIO? *(Section 7.1)*			
67.	Have all types of "remote control" (e.g., PCAnywhere) been prohibited except where they are specifically, and uniquely approved by the agency CIO? *(Section 7.1)*			
68.	Have all network-monitoring tools been prohibited except where they are specifically, and uniquely approved by the agency CIO? *(Section 7.1)*			
69.	Are dial-in users required to use an id that is different from their application or network user id? *(Section 7.1)*			
70.	Is the call pickup for modems set to a minimum of six (6) rings? *(Section 7.1)*			
71.	Are dial-in users restricted to accessing only specific applications or servers (i.e., do not have access to the entire network)? *(Section 7.1)*			
72.	Is an annual review performed for all dial-in users? *(Section 7.1)*			
73.	Are all firewalls configured to block unnecessary services? *(Section 7.3)*			
74.	Are security updates and patches applied to all network devices in a timely manner? *(Section 7.3)*			
75.	Has the agency documented and implemented a severity and escalation list based upon anticipated events that includes immediate response capability when appropriate? *(Section 7.4)*			

	Physical Security Standard			
76.	Have all IT areas been secured with controls commensurate to the risks? *(Section 8, 8.1, and 8.5)*			
77.	Has a process been implemented to ensure the secure storage, reuse, and/or destruction of storage media? *(Section 8, 8.2, 8.3, and 8.4)*			
	Microcomputer/PC/Laptop Security Standard			
78.	Have all microcomputers (i.e., workstations, desktop computers, laptop computers, PDAs, and other portable devices) been secured against unauthorized access? *(Section 9)*			
79.	Do all microcomputers that store, process, and/or access non-public information require a unique user id and password for access? *(Section 9.1)*			
80.	Is virus protection installed on all microcomputers? *(Section 9.1)*			
81.	Are the virus definitions updated weekly? *(Section 9.1)*			
82.	Are virus definitions updated immediately when circumstances warrant such action (e.g., to control the spread of a new virulent strain)? *(Section 9.1)*			
83.	Are microcomputer and/or the servers configured to run checks for viruses at startup and to operate in memory resident mode to check for viruses during normal processing? *(Section 9.1)*			
84.	Are the networks configured to prevent connection to microcomputers unless the latest version of the virus product update has been installed and running? *(Section 9.1)*			
85.	Has the agency established procedures to ensure compliance with software licensing and use? *(Section 9.2)*			
86.	Are laptops and mobile computing devices prohibited from accessing or storing nonpublic information unless approved in writing by the Information Custodian? *(Section 9.4)*			
87.	Is personally owned data processing equipment (i.e., not owned by the State) prohibited from accessing systems with nonpublic information? *(Section 9.5)*			
	Encryption Standard			
88.	Is encryption utilized to protect all information classified as NON-PUBLIC INFORMATION-High when it is stored or transmitted? *(Section 10)*			
89.	Do all IT Systems employing encryption comply with applicable Federal Information Processing Standards? *(Section 10)*			
90.	Are all cryptographic keys secure from unauthorized access? *(Section 10)*			
91.	Have all Public Key Cryptography methods been approved by the State CIO and the Data Security Committee? *(Section 10 and 10.2)*			
92.	Do all cryptographic keys have a designated, unique owner? *(Section 10.1)*			

93.	Are master keys changed at least annually? *(Section 10.1)*			
94.	Are key encrypting keys (e.g., asymmetric encrypting a symmetric) changed at least every six (6) months? *(Section 10.1)*			
95.	Are link encrypting keys changed at least every thirty (30) days? *(Section 10.1)*			
96.	Are keys distributed in a secure manner? *(Section 10.1)*			
97.	Are default cryptographic keys prohibited except for emergency recovery? *(Section 10.1)*			
98.	Has an associated scope of use be documented for every public key and certificate? *(Section 10.2)*			
99.	Has a secure process been implemented for issuing digital certificates? *(Section 10.2)*			
	IT Information Security Deviation/Risk Acceptance Standard			
100.	Has an IT Information Security Deviation been completed for all instances on non-compliance with the State IT Security Policy? *(Section 11)*			
101.	Has the Information Custodian renewed applicable IT Information Security Deviations that are still enforce after 12 months? *(Section 11)*			
	Use of Electronic Communications Standard			
102.	Has the agency ensured that all employees/contractors understand that the use of the Internet, E-mail and other State computing equipment, networks and communication facilities are provided to meet their job functions and as such all information is State property and is not subject to privacy? *(Section 12)*			

14 Record of Revisions

Issue	Date	Section Modified	Description
Policy issued	June 6, 2003	N/A	N/A
Revision 1.1	July 24, 2003	Section 7 Paragraph 7.2 Banner	Banner Text modified